Srinivas Piskala Ganesh Babu
Spg349 and N13138339

Firewalling

2.1. Part A

For outgoing traffic (from 10.20.111.0/24 to 10.10.111.0/24) - your internal machine should be able to communicate with the external network and the external machines without restrictions.

For incoming traffic (from the 10.10.111.0/24 to the 10.20.111.0/24) - all incoming connection requests should be rejected with the following exceptions:

1. 1) [10 pts] The internal machine should respond to a ping from 10.10.111.0/24
2. 2) [20 pts] The internal machine (10.20.111.2) should accept all incoming SSH and http requests from 10.10.111.0/24
3. 3) [20 pts] The internal machine should accept telnet connections from the BT Machine only.
4. 4) [10 pts] The **internal router** should accept pings from the BT machine only.

Based on the conditions mentioned above, The Rules Configured for the IP Tables are as follows

```
### OUTGOING TRAFFIC FROM 10.20.111.0
# OutGoing Traffic From Internal Machine - ALL Accept

iptables -A FORWARD -s 10.20.111.2 -d 10.10.111.0/24 -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT

# Output to External Network
iptables -A OUTPUT -s 10.20.111.0/24 -d 10.10.111.0/24 -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT

### INCOMING TRAFFIC

# 1. PING from External to Internal Machine
iptables -A FORWARD -s 10.10.111.0/24 -d 10.20.111.2 -p icmp -j ACCEPT

# 2. Internal Machine - SSH and HTTP Connection from External Network
# To Internal Machine - SSH and HTTP from any External Machines - Only NEW
Connections
iptables -A FORWARD -s 10.10.111.0/24 -d 10.20.111.2 -m state --state
NEW,ESTABLISHED,RELATED -p tcp --dport 80 -j ACCEPT

iptables -A FORWARD -s 10.10.111.0/24 -d 10.20.111.2 -m state --state
NEW,ESTABLISHED,RELATED -p tcp --dport 22 -j ACCEPT

# 3. Internal Machine accpets only Telnet from BT5
# To Internal Machine - TELNET from only BT5
iptables -A FORWARD -s 10.10.111.107 -d 10.20.111.2 -p tcp --dport 23 -j
ACCEPT
```

```
# 4. Internal Router Accepts PING from only BT5
# PING from only BT5 to Router
iptables -A INPUT -s 10.10.111.107 -p icmp -j ACCEPT

# Stateful Setting - Accept Only Established Connection Traffic - Handle
reply of Outgoing Connection from Internal Machine
iptables -A FORWARD -s 10.10.111.0/24 -m state --state ESTABLISHED,RELATED -j
ACCEPT
iptables -A INPUT -s 10.10.111.0/24 -m state --state ESTABLISHED,RELATED -j
ACCEPT

# Reject Everything Else
iptables -A FORWARD -s 10.10.111.0/24 -j REJECT
iptables -A INPUT -s 10.10.111.0/24 -j REJECT

### DISPLAY
# Show Tables
iptables -nL
```

The Output of the IPTable is as follows at the INTERNAL Router: (Full Screen Placed Next)

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     icmp --  10.10.111.107        0.0.0.0/0
ACCEPT     all  --  10.10.111.0/24       0.0.0.0/0           state RELATED,ESTABLISHED
REJECT     all  --  10.10.111.0/24       0.0.0.0/0           reject-with icmp-port-unreachable

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  10.20.111.2          10.10.111.0/24      state NEW,RELATED,ESTABLISHED
ACCEPT     icmp --  10.10.111.0/24       10.20.111.2
ACCEPT     tcp  --  10.10.111.0/24       10.20.111.2         state NEW,RELATED,ESTABLISHED tcp
dpt:80
ACCEPT     tcp  --  10.10.111.0/24       10.20.111.2         state NEW,RELATED,ESTABLISHED tcp
dpt:22
ACCEPT     tcp  --  10.10.111.107        10.20.111.2         tcp dpt:23
ACCEPT     all  --  10.10.111.0/24       0.0.0.0/0           state RELATED,ESTABLISHED
REJECT     all  --  10.10.111.0/24       0.0.0.0/0           reject-with icmp-port-unreachable

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  10.20.111.0/24       10.10.111.0/24      state NEW,RELATED,ESTABLISHED
```

- Outgoing Connections are all enabled with OUTPUT (for Internal Router) and FORWARD (for internal machine)
    - Respective Stateful Connections for “ESTABLISHED and RELATED” have been enabled to perform outgoing connections without any interference
- Incoming Connections are handled using INPUT (for Internal Router) and FORWARD (For Internal Machine)
    - Respective Stateful to be NEW, ESTABLISHED and RELATED have been added with source IP filters based on the questions above
- All the other connections are rejected which is placed in the final place to hit once all the other rules above fails

IPtables Full Configuration Screens:

➔ **IPtable Firewall Configuration Screens**

- **INPUT Chain**

```
router:~#
router:~#
router:~#
router:~#
router:~#
router:~#
router:~#
router:~# iptables -nL INPUT
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     icmp --  10.10.111.107        0.0.0.0/0
ACCEPT     all  --  10.10.111.0/24       0.0.0.0/0           state RELATED,ESTAB
LISHED
REJECT     all  --  10.10.111.0/24       0.0.0.0/0           reject-with icmp-po
rt-unreachable
router:~#
router:~#
router:~#
router:~#
router:~#
router:~#
router:~#
router:~# _
```

- **FORWARD and OUTPUT Chain**

```
ACCEPT     all  --  10.10.111.0/24       0.0.0.0/0           state RELATED,ESTAB
LISHED
REJECT     all  --  10.10.111.0/24       0.0.0.0/0           reject-with icmp-po
rt-unreachable

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  10.20.111.2          10.10.111.0/24      state NEW,RELATED,E
STABLISHED
ACCEPT     icmp --  10.10.111.0/24       10.20.111.2
ACCEPT     tcp  --  10.10.111.0/24       10.20.111.2         state NEW,RELATED,E
STABLISHED tcp dpt:80
ACCEPT     tcp  --  10.10.111.0/24       10.20.111.2         state NEW,RELATED,E
STABLISHED tcp dpt:22
ACCEPT     tcp  --  10.10.111.107        10.20.111.2         tcp dpt:23
ACCEPT     all  --  10.10.111.0/24       0.0.0.0/0           state RELATED,ESTAB
LISHED
REJECT     all  --  10.10.111.0/24       0.0.0.0/0           reject-with icmp-po
rt-unreachable

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  10.20.111.0/24       10.10.111.0/24      state NEW,RELATED,E
STABLISHED
router:~#
```

Network Security Lab – 7 = IPTables

Srinivas Piskala Ganesh Babu
Spg349 and N13138339

Screenshots of the results:

➔ **Outgoing Traffic from the Internal Machine:**

- **PING to Outside Network**

```
vlab-debian:~#
vlab-debian:~#
vlab-debian:~# ping 10.10.111.107
PING 10.10.111.107 (10.10.111.107) 56(84) bytes of data.
64 bytes from 10.10.111.107: icmp_seq=1 ttl=63 time=12.7 ms
64 bytes from 10.10.111.107: icmp_seq=2 ttl=63 time=4.36 ms
64 bytes from 10.10.111.107: icmp_seq=3 ttl=63 time=3.59 ms
64 bytes from 10.10.111.107: icmp_seq=4 ttl=63 time=4.02 ms
c64 bytes from 10.10.111.107: icmp_seq=5 ttl=63 time=3.97 ms
64 bytes from 10.10.111.107: icmp_seq=6 ttl=63 time=3.68 ms
^C
--- 10.10.111.107 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5019ms
rtt min/avg/max/mdev = 3.596/5.394/12.722/3.287 ms
vlab-debian:~# ping 10.10.111.1
PING 10.10.111.1 (10.10.111.1) 56(84) bytes of data.
64 bytes from 10.10.111.1: icmp_seq=1 ttl=63 time=7.27 ms
64 bytes from 10.10.111.1: icmp_seq=2 ttl=63 time=4.10 ms
64 bytes from 10.10.111.1: icmp_seq=3 ttl=63 time=4.46 ms
64 bytes from 10.10.111.1: icmp_seq=4 ttl=63 time=3.60 ms
^C
--- 10.10.111.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3010ms
rtt min/avg/max/mdev = 3.602/4.863/7.279/1.428 ms
vlab-debian:~# _
```

- **SSH to Outside Network – Internal Machine to Student Linux Machine Outside**

```
vlab-debian:~#
vlab-debian:~#
vlab-debian:~#
vlab-debian:~# ssh student@10.10.111.106
The authenticity of host '10.10.111.106 (10.10.111.106)' can't be established.
RSA key fingerprint is c3:7d:70:74:f8:0d:d4:16:47:39:0b:41:10:0a:2f:46.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.111.106' (RSA) to the list of known hosts.
student@10.10.111.106's password:
Linux linux-machine 2.6.26-2-amd64 #1 SMP Tue Mar 9 22:29:32 UTC 2010 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Fri May 14 20:29:44 2010 from 10.10.111.1
xset:  unable to open display ""
student@linux-machine:~$ exit
logout
Connection to 10.10.111.106 closed.
vlab-debian:~#
vlab-debian:~#
```

➔ **Incoming Connections:**

- **Internal Machine PING from 10.10.111.0 Network – PING**
  - **From 10.10.111.1**

```
router:~#
router:~#
router:~#
router:~#
router:~#
router:~#
router:~#
router:~# ping 10.20.111.2
PING 10.20.111.2 (10.20.111.2) 56(84) bytes of data.
64 bytes from 10.20.111.2: icmp_seq=1 ttl=63 time=4.10 ms
64 bytes from 10.20.111.2: icmp_seq=2 ttl=63 time=3.80 ms
64 bytes from 10.20.111.2: icmp_seq=3 ttl=63 time=4.36 ms
64 bytes from 10.20.111.2: icmp_seq=4 ttl=63 time=4.29 ms
64 bytes from 10.20.111.2: icmp_seq=5 ttl=63 time=3.55 ms
64 bytes from 10.20.111.2: icmp_seq=6 ttl=63 time=3.77 ms
^C
--- 10.20.111.2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5021ms
rtt min/avg/max/mdev = 3.555/3.983/4.369/0.294 ms
router:~#
router:~#
router:~#
router:~#
router:~#
router:~#
```

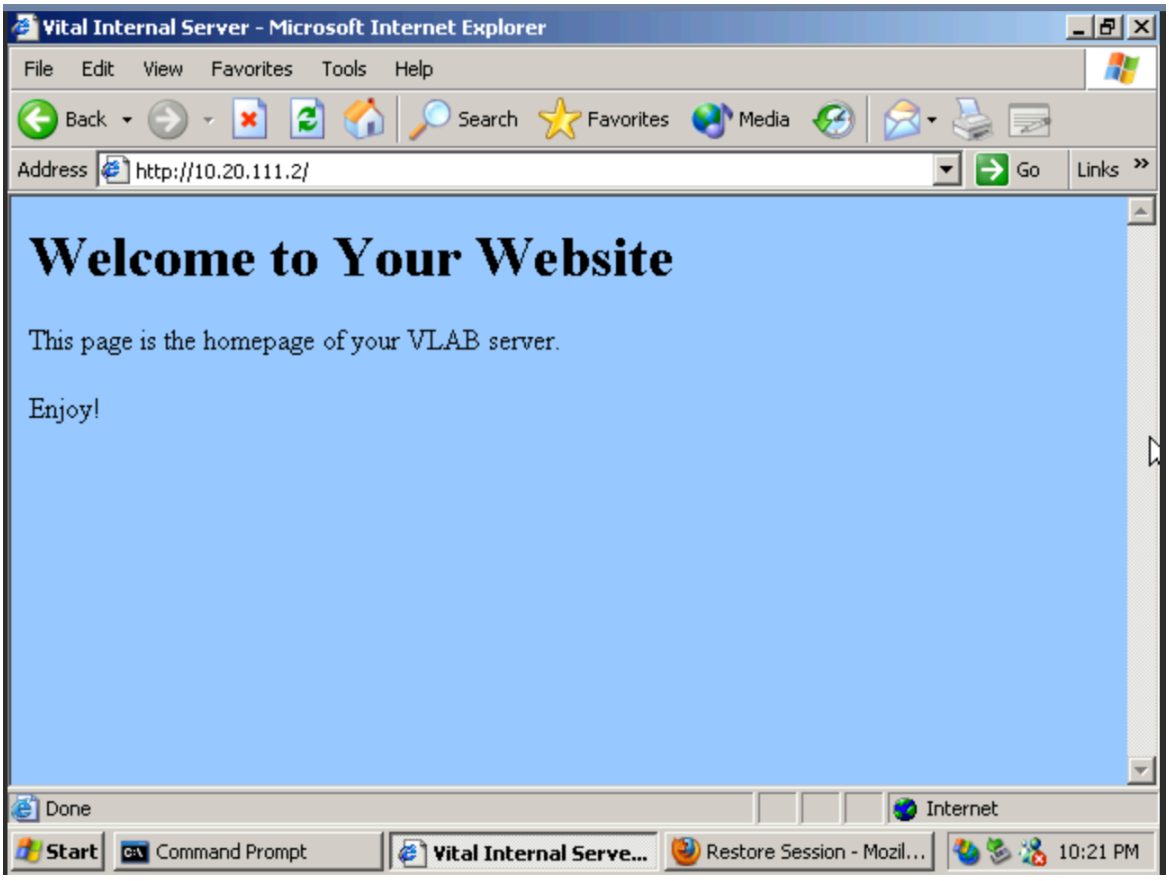
  - **From 10.10.111.110 – Windows Machine**

```
Command Prompt
C:\Documents and Settings\poly>
C:\Documents and Settings\poly>
C:\Documents and Settings\poly>
C:\Documents and Settings\poly>
C:\Documents and Settings\poly>
C:\Documents and Settings\poly>
C:\Documents and Settings\poly>
C:\Documents and Settings\poly>
C:\Documents and Settings\poly>
C:\Documents and Settings\poly>
C:\Documents and Settings\poly>
C:\Documents and Settings\poly>
C:\Documents and Settings\poly>
C:\Documents and Settings\poly>
C:\Documents and Settings\poly>ping 10.20.111.2

Pinging 10.20.111.2 with 32 bytes of data:

Reply from 10.20.111.2: bytes=32 time=11ms TTL=63
Reply from 10.20.111.2: bytes=32 time=6ms TTL=63
Reply from 10.20.111.2: bytes=32 time=5ms TTL=63
Reply from 10.20.111.2: bytes=32 time=4ms TTL=63

Ping statistics for 10.20.111.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 11ms, Average = 6ms

C:\Documents and Settings\poly>
C:\Documents and Settings\poly>
C:\Documents and Settings\poly>
C:\Documents and Settings\poly>
C:\Documents and Settings\poly>
C:\Documents and Settings\poly>
Start  Command Prompt  10:15 PM
```

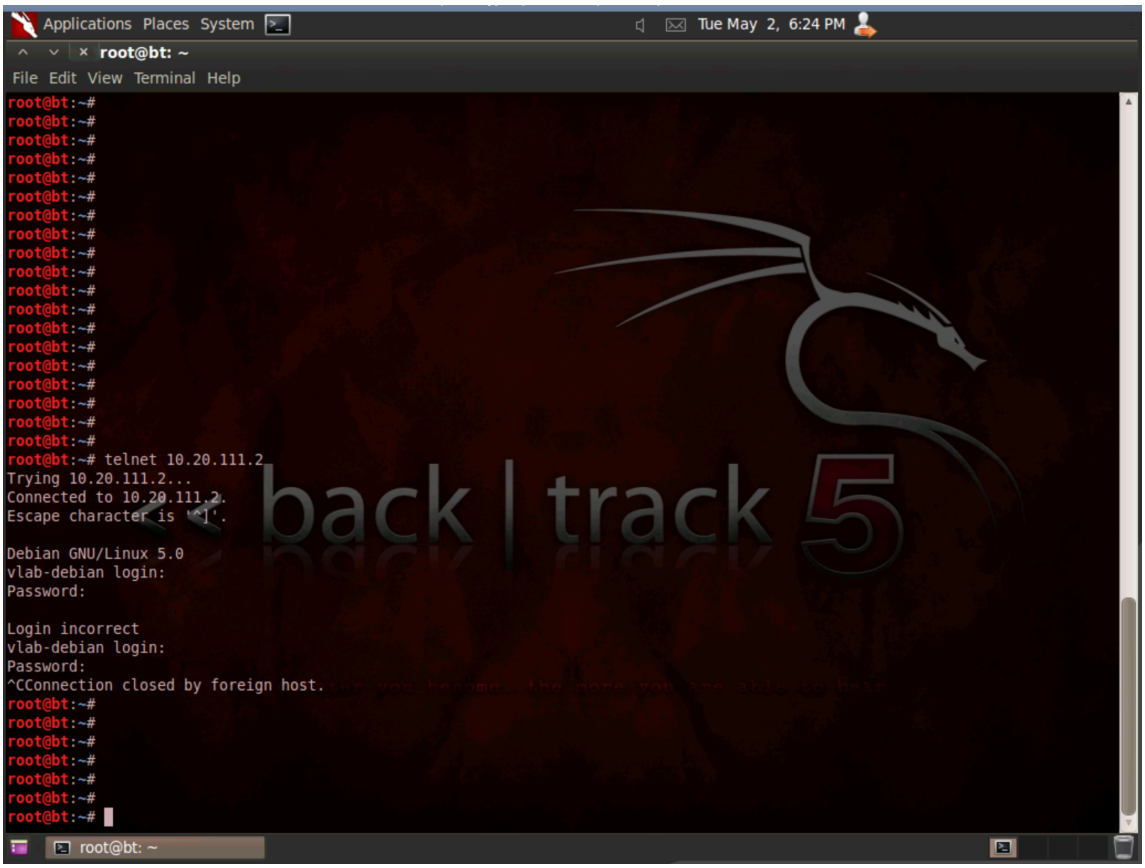
- **SSH and HTTP from 10.10.111.0 Network - SSH**
  - **SSH From External Router – 10.10.111.1**

```
router:~#
router:~#
router:~#
router:~#
router:~# ssh root@10.20.111.2
root@10.20.111.2's password:
Linux vlab-debian 2.6.26-2-amd64 #1 SMP Thu Nov 5 02:23:12 UTC 2009 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue May  2 17:27:17 2017
vlab-debian:~#
vlab-debian:~#
vlab-debian:~#
vlab-debian:~#
vlab-debian:~#
vlab-debian:~#
vlab-debian:~# exit
logout
Connection to 10.20.111.2 closed.
router:~#
```

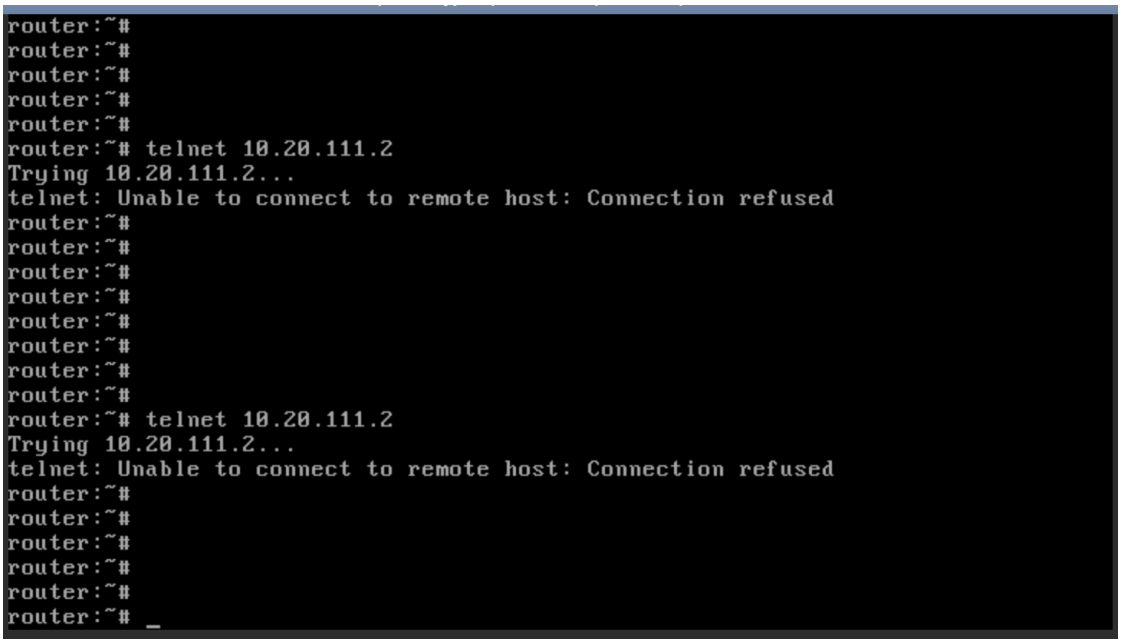
  - **HTTP from Windows Machine - HTTP**

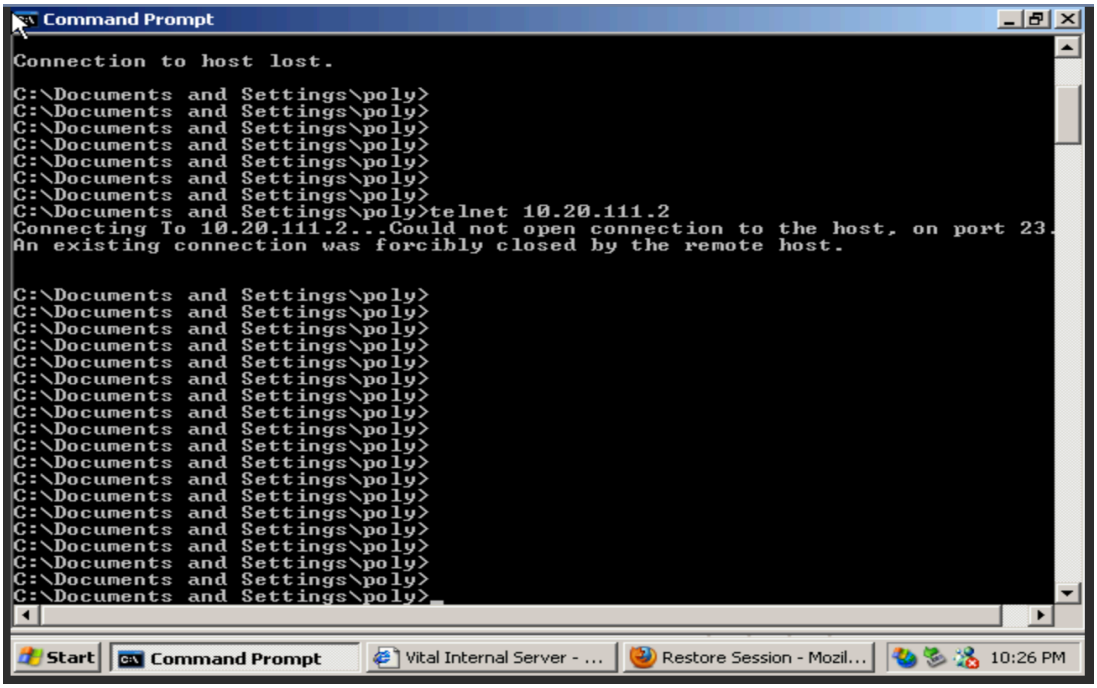


- **Internal Machine - Telnet from BT5 Only - TELNET**
  - **Telnet From BT5 to the Internal Machine**



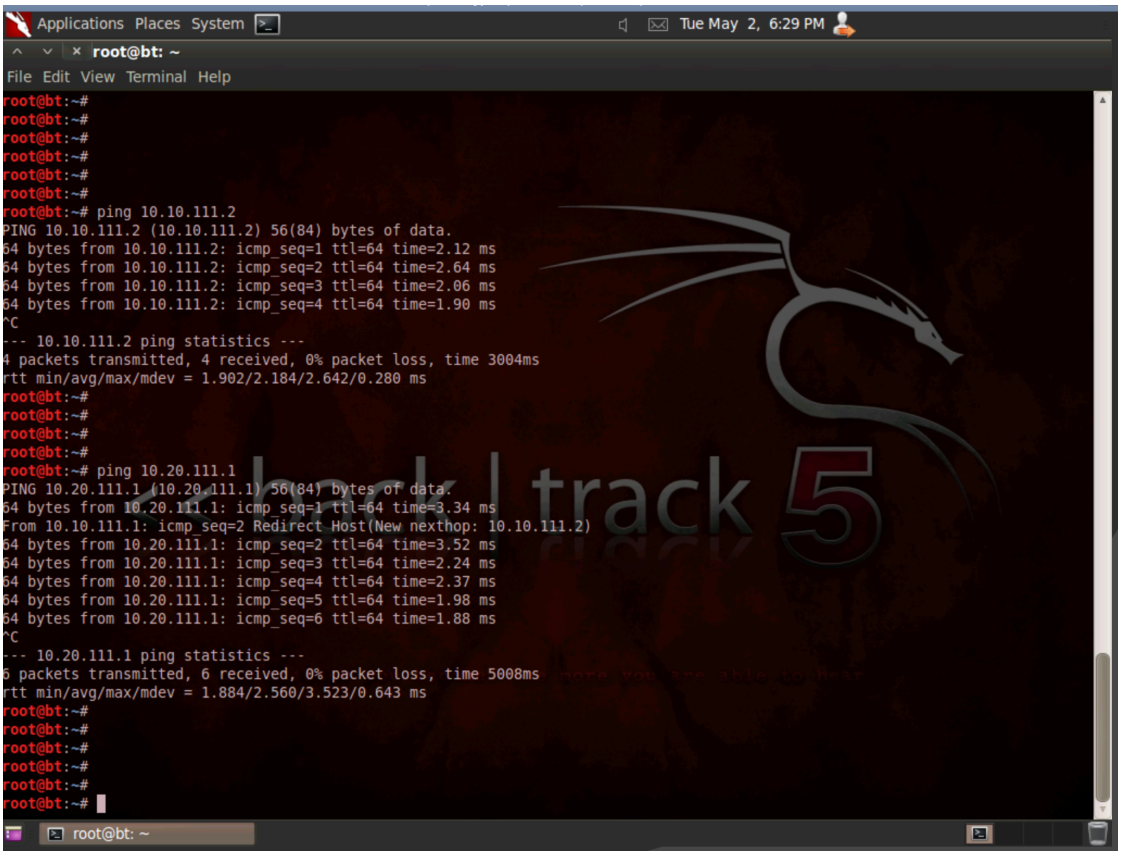
  - **Telnet from Other Machines**



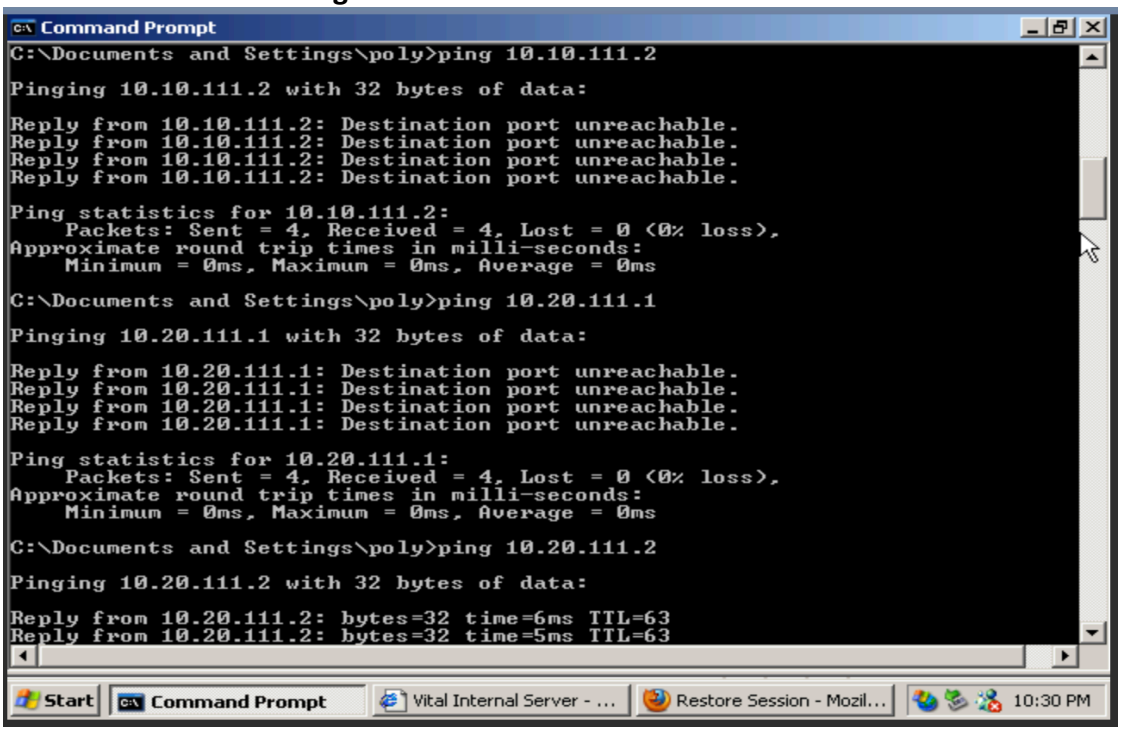


- **Internal Router - Ping from BT5 Only**

- **Ping from BT5 to the Internal Router - Both the interface – 10.10.111.2 and 10.20.111.1**

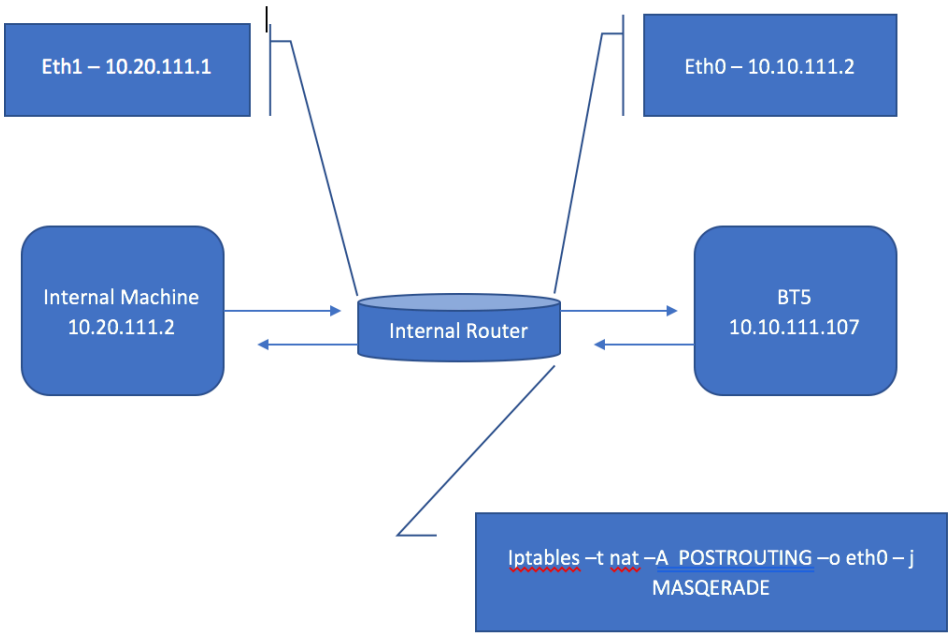


- **Ping from Windows to the Internal Router**



PartB:

[20 pts] Use the MASQUERADE target to perform the NAT



Network Security Lab – 7 = IPTables

Srinivas Piskala Ganesh Babu
Spg349 and N13138339

Rule:

```
### NAT Rule to MASQUERADE the Source IP to a 10.10.111.x
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
### Show NAT Table
iptables -t nat -nL
```

Results of the IP Table for NAT:

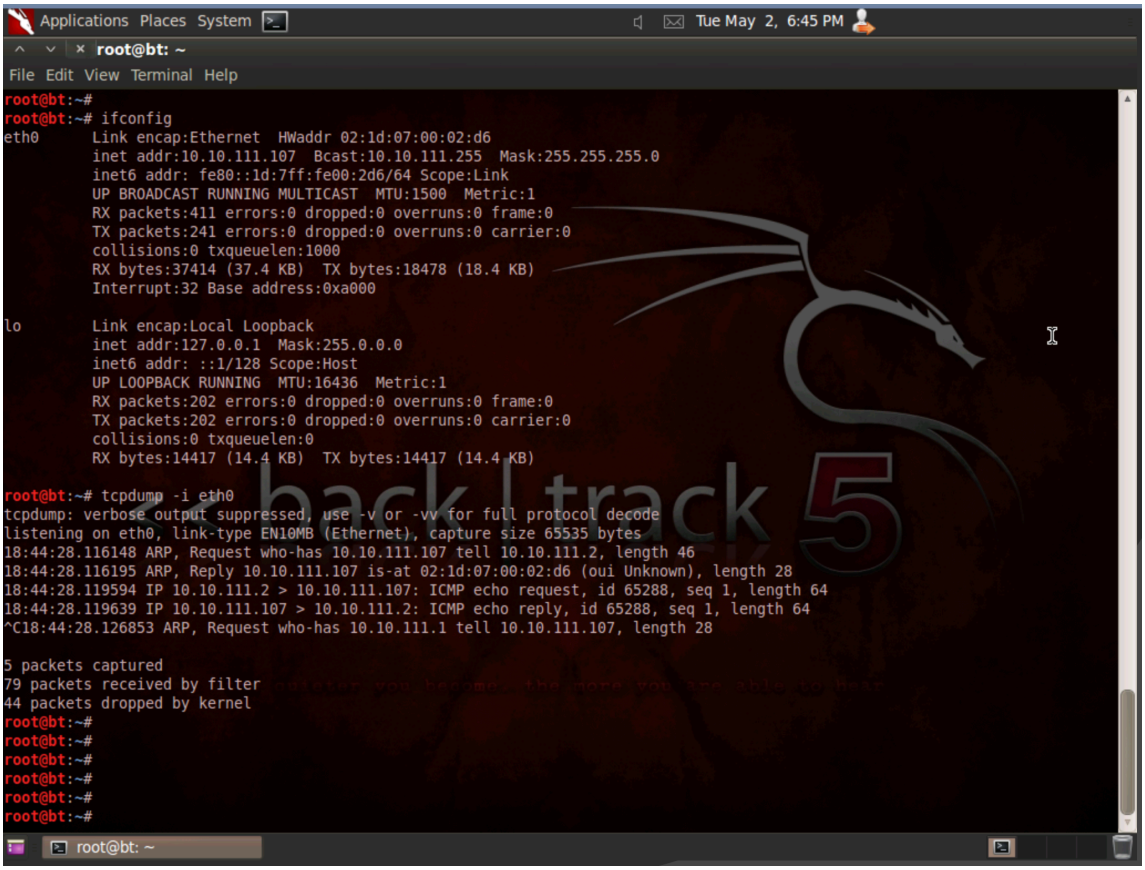
```
~
~
router:~# iptables -t nat -F
router:~# iptables -F
router:~#
router:~# ./nat.txt
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  all  --  0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
router:~#
router:~#
router:~#
router:~#
router:~#
router:~#
router:~#
router:~#
router:~#
router:~# _
```

Screenshots:

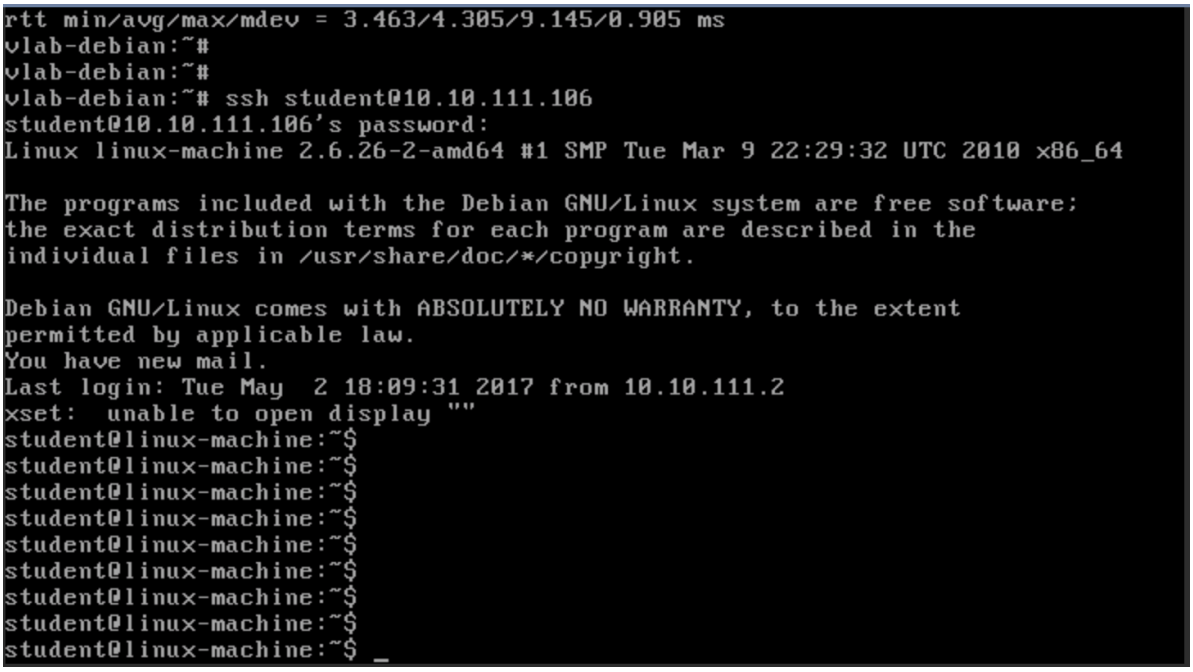
*** Initiated Ping from Internal Machine and Packet Capture (TCPDump) at BT5**

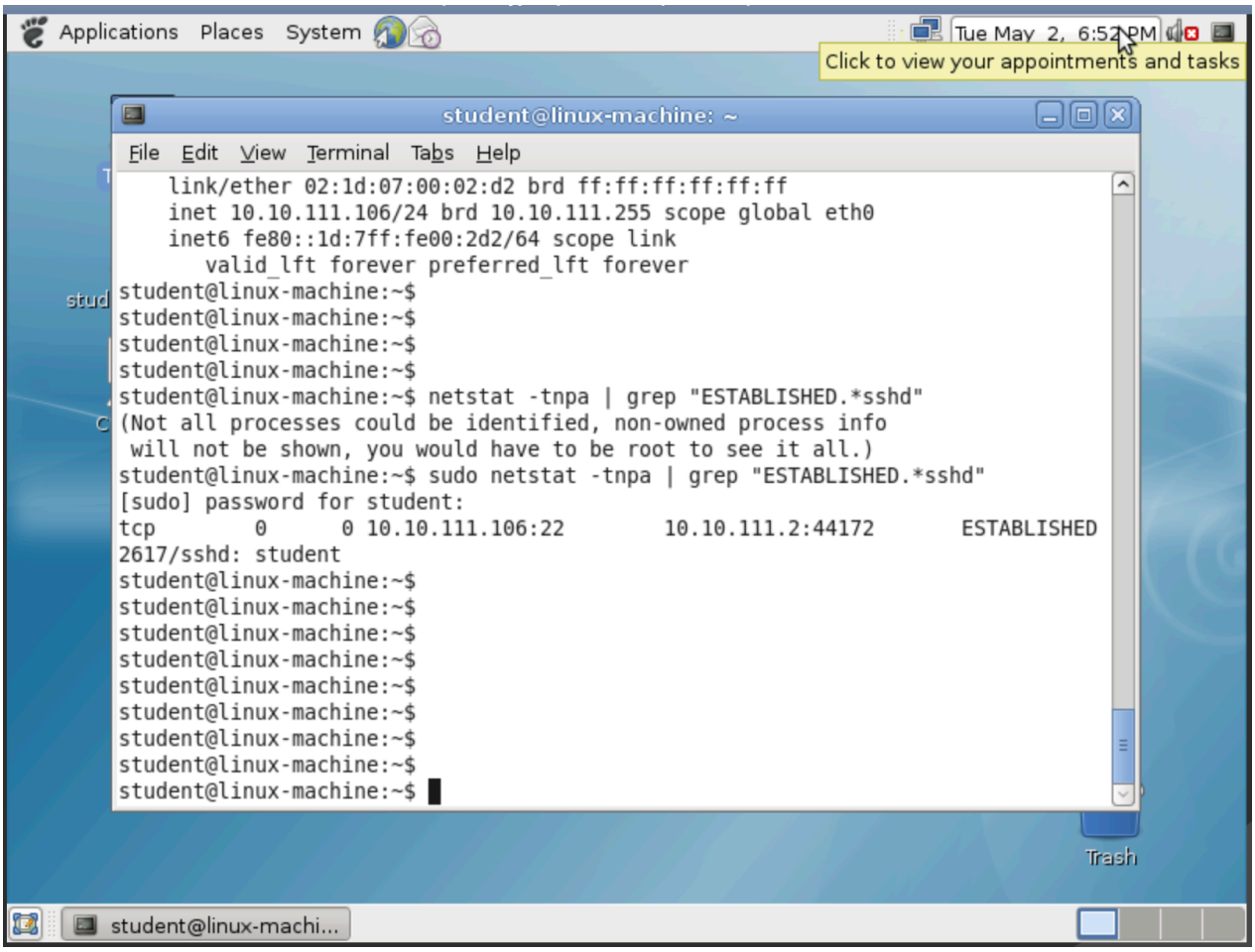
```
64 bytes from 10.10.111.107: icmp_seq=15 ttl=63 time=4.01 ms
64 bytes from 10.10.111.107: icmp_seq=16 ttl=63 time=3.84 ms
64 bytes from 10.10.111.107: icmp_seq=17 ttl=63 time=4.53 ms
64 bytes from 10.10.111.107: icmp_seq=18 ttl=63 time=4.33 ms
64 bytes from 10.10.111.107: icmp_seq=19 ttl=63 time=3.58 ms
64 bytes from 10.10.111.107: icmp_seq=20 ttl=63 time=4.26 ms
64 bytes from 10.10.111.107: icmp_seq=21 ttl=63 time=3.46 ms
64 bytes from 10.10.111.107: icmp_seq=22 ttl=63 time=4.17 ms
64 bytes from 10.10.111.107: icmp_seq=23 ttl=63 time=4.49 ms
64 bytes from 10.10.111.107: icmp_seq=24 ttl=63 time=4.02 ms
64 bytes from 10.10.111.107: icmp_seq=25 ttl=63 time=4.10 ms
64 bytes from 10.10.111.107: icmp_seq=26 ttl=63 time=4.37 ms
64 bytes from 10.10.111.107: icmp_seq=27 ttl=63 time=3.79 ms
64 bytes from 10.10.111.107: icmp_seq=28 ttl=63 time=3.88 ms
64 bytes from 10.10.111.107: icmp_seq=29 ttl=63 time=4.14 ms
64 bytes from 10.10.111.107: icmp_seq=30 ttl=63 time=4.33 ms
64 bytes from 10.10.111.107: icmp_seq=31 ttl=63 time=4.18 ms
64 bytes from 10.10.111.107: icmp_seq=32 ttl=63 time=3.97 ms
64 bytes from 10.10.111.107: icmp_seq=33 ttl=63 time=4.24 ms
64 bytes from 10.10.111.107: icmp_seq=34 ttl=63 time=4.53 ms
^C
--- 10.10.111.107 ping statistics ---
34 packets transmitted, 34 received, 0% packet loss, time 33131ms
rtt min/avg/max/mdev = 3.463/4.305/9.145/0.905 ms
vlab-debian:~#
```

TCPDump – shows the IP as 10.10.111.2 – Internal Router Outside Interface



-> SSH Connection from Internal Machine To Student Linux Machine





The established SSH connection of the student Linux machine shows the NAT IP when a connect is made from the Internal Machine.

SSH Session Open = 10.10.111.2 (The Router Outer Interface – NAT IP)

The TCPDump packet capture made during PING request from the Internal Machine and the SSH Session Open when SSH Connection is made from the Internal Machine shows both the IPs to 10.10.111.2 which is the Outside Interface of the Internal Router. The Source IP – 10.20.111.2 is changed successfully.

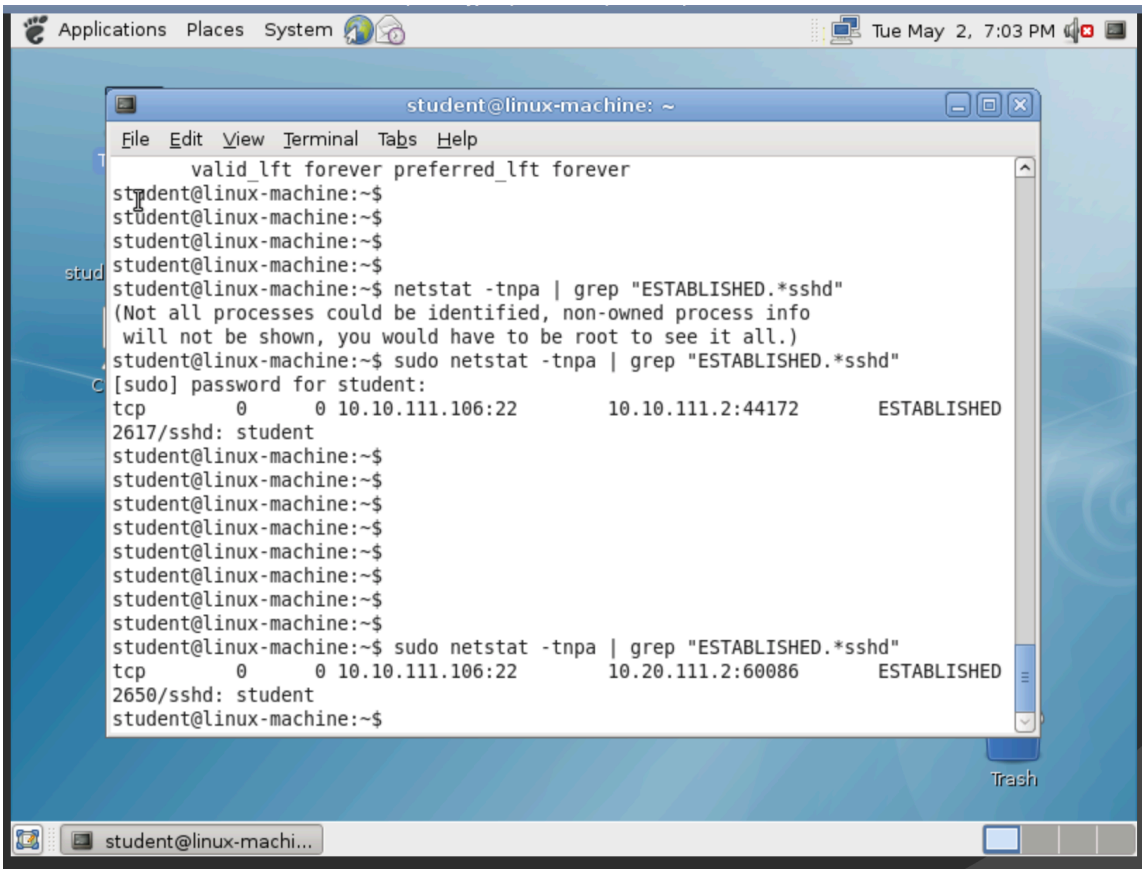
Both Ping and the SSH Connections show the Router IP (Outside Interface) – 10.10.111.2 as the source IP when the connection is initiated from the Internal Machine – 10.20.111.2. Thus, NAT has successfully been installed at the Internal Router.

Network Security Lab – 7 = IPTables

Srinivas Piskala Ganesh Babu
Spg349 and N13138339

Once the IPtable is flushed, results in IP to be reverted to Machine IP (No NAT)

```
router:~#
router:~#
router:~#
router:~#
router:~#
router:~#
router:~#
router:~#
router:~# iptables -t nat -F
router:~# iptables -F
router:~# iptables -t nat -nL
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
router:~#
router:~#
router:~#
router:~#
router:~#
router:~#  _
```



Srinivas Piskala Ganesh Babu
Spg349 and N13138339

2.3.Part C

Answer the following questions:
1) [5 pts] In your own words describe how iptables works.

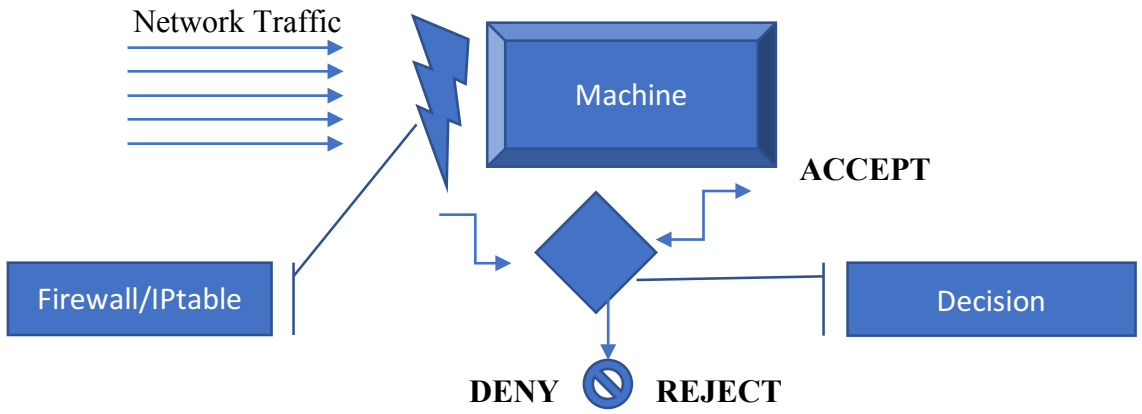
Iptables define a **set of rules** with which the **network traffic is compared** to **make a decision** of accept or drop or reject them respectively. The Iptable rules are segregated in the form of INPUT, OUTPUT and FORWARD chain based on the packet flow and the Designation/Source address.

These packet rules constitute a pattern to defend or filter out ambiguous traffic and allow only legitimate traffic based on various scenarios.

When a Packet is received by the device, there occurs a decision to be made with respect to what is considered as legitimate and filter out ambiguous traffic.

When a packet is received,

1. The Iptable rules are looked upon.
2. Each Rule in the IP Table is compared to the packet contents
3. If the Rule matches, a decision is arrived at to ACCEPT or DROP the packet



2) [5 pts] What is the difference between input, output and forward chains?

INPUT Chain – This rule hits when the incoming or destination address of the packet is its own IP address where the firewall is running. Applied to the packets which are received by the machine for itself. (Destined to itself)

OUTPUT Chain - This rule hits when the outgoing or source address of the packet is its own IP address where the firewall is running. Applies to the packets which are created by the machine itself

FORWARD Chain – This rule is hit when both the destination and source address differ from that of own ipaddress where the Iptable/Firewall is running. (Packets that need to be routed through)

3) [5 pts] What is the difference is between deny, reject and accept?

Deny – The Request is denied and the packet is dropped

Reject – The Request is denied and an ICMP reject is returned

Accept – The Request is granted access and the packet is forwarded or processed

4) [5 pts] Do some research and find some three alternative network based firewalls. List and describe the pros and cons of each when compared to iptables. The alternative can be commercial, opensource or even a stand alone appliance.

- **Windows Firewall:**
  - **OS : Windows**
  - **Type : Proprietary**
  - **Cost : Comes with only Windows Software**
  - **Special Features:**
    - By Default blocks ping. (Tested with Win10)
  - Pros:
    - Better Notification Features
    - Better GUI for rules creation and maintenance
    - The default security policy is efficient to block attacks
  - Cons:
    - Difficult to handle complex network
    - Rule creations are not very easy as iptables
    - NAT capabilities are not present
- **Commodo Internet Security:**
  - **OS : Windows**
  - **Type: Proprietary**
  - **Cost : Free**
  - **Special Features:**
    - **Sandbox –** Isolates and containerizes application for better security
  - **Pros:**
    - **Sandbox –** Isolates and protects browsers by isolating them
    - **More than just a firewall** - Contains anti rootkits, bot protect features
  - **Cons:**
    - Adds a lot of **overhead** due to extra features and makes the process slower
- **CISCO FirePower:**
  - **OS: Cisco Propriety Operating System – IOS**

- **Type: Propriety**
- **Cost: Included in CISCO Devices – StandALone**
- **Special Features:**
  - Firewall with Intrusion and Malware Prevention
  - Effective to handle complex and huge traffic
- Pros:
  - Comes with effective Application Control, Malware Protect and URL Filtering features
  - Effectively handles huge traffic as well as different types of traffic
  - Advanced comparison capabilities with packet sizes and other criterions
- Cons:
  - Mostly concentrated on FORWARD chains only